E

Email Attacks: Types, Warning Signs, and Response

Email attacks include phishing, business email compromise, malicious attachments, account takeover, and OAuth abuse. Learn how to spot and stop them.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
4 min

CONTENTS

In this guide

01 What is an email attack?
02 Common types of email attack
03 Warning signs to check
04 What SPF, DKIM, and DMARC do
05 How to prevent email attacks
06 What to do after a suspicious email
07 Email attack vs. spam

Quick answer: Email attacks use messages or compromised mailboxes to steal credentials or money, deliver malware, or gain trusted access. Treat urgent payment changes, unexpected sign-ins, unusual attachments, QR codes, and permission requests as high risk. Verify important requests through a known second channel and report suspicious messages without clicking or replying.

01 What is an email attack?

An email attack is any malicious campaign that uses email as the delivery path or abuses a mailbox's trusted identity. Some attacks contain a harmful file or link. Others use no malware at all: a convincing conversation can persuade an employee to change bank details, disclose information, buy gift cards, or approve an attacker-controlled cloud application.

02 Common types of email attack

- **Phishing:** a broad message impersonates a service and directs recipients to a fake sign-in or harmful file.
- **Spear phishing:** a tailored message uses details about one person, role, project, or supplier.
- **Business email compromise (BEC):** an attacker impersonates an executive, vendor, or lawyer to redirect payments or obtain sensitive data.
- **Account takeover and thread hijacking:** a real mailbox is compromised, then used to reply inside an existing conversation.
- **Malicious links, attachments, and QR codes:** the message sends the victim to credential theft, malware, or a fake support process.
- **OAuth consent phishing:** a cloud application requests mailbox, files, contacts, or identity permissions instead of stealing a password.
- **Spoofing and lookalike domains:** the display name or address resembles a trusted sender, sometimes with a small spelling change.

03 Warning signs to check

Look at the complete sender address, reply-to address, destination of links, and the business context. Be cautious when a message introduces secrecy, urgency, changed payment instructions, an unfamiliar login page, a protected archive with a password, or a document that asks you to enable macros. A QR code hides its destination from normal link previews, so verify the request before scanning.

Good grammar does not prove legitimacy, and a familiar sender is not enough: attackers can compromise real mailboxes. Unexpected changes in tone, timing, invoice details, or process are often more useful than spelling mistakes.

04 What SPF, DKIM, and DMARC do

SPF authorizes sending systems, DKIM signs message content and selected headers, and DMARC tells receiving systems how to evaluate alignment and report failures. Correct deployment reduces direct domain spoofing, but it does not stop lookalike domains, compromised accounts, or every forwarded message. Email authentication should support, not replace, identity controls and verification procedures.

05 How to prevent email attacks

1. Use phishing-resistant multifactor authentication where available and protect mailbox recovery methods.
2. Configure SPF, DKIM, and DMARC, monitor reports, and tighten policy after confirming legitimate senders.
3. Require independent confirmation for payment, payroll, password reset, and bank-detail changes using a known phone number or approved workflow.
4. Disable legacy authentication, restrict automatic forwarding, and alert on unusual inbox rules and OAuth grants.

5. Filter risky attachments and URLs, sandbox content when appropriate, and keep endpoints and office software patched.
6. Make reporting easy and review simulations as coaching, not punishment.

06 What to do after a suspicious email

If you did not interact, report the message through the approved channel and leave it intact for analysis. Do not forward it normally if that could activate content; use the organization's reporting function. If you entered a password, change it from a clean device, revoke active sessions, reset multifactor methods if needed, and tell the security team what was entered.

If you opened a suspicious attachment or installed software, disconnect the device from the network without powering it off unless responders instruct otherwise. Preserve the email and endpoint evidence. If money was sent, contact the financial institution immediately through a verified number and request a recall or hold; then notify law enforcement or the appropriate fraud reporting service. Speed matters in payment fraud.

07 Email attack vs. spam

Spam is unsolicited bulk email and may be merely unwanted. An email attack has a harmful objective such as theft, compromise, or fraud. A message can be both spam and an attack, but a highly targeted BEC message may be sent to only one person and never look like bulk spam.

NEED MORE HELP?

We are here when the guide is not enough.

Visit the Gridinsoft Support Center for current product guidance or submit a support request with the details of your case.

Open this guide online at support.gridinsoft.com